The Claims:

Applicant reserves the right to pursue the subject matter of the original claims in this application and in other applications. This listing of claims will replace all prior versions, and listings, of claims in the application. No new matter is introduced by this amendment and the amendments to the claims are fully supported by the original specification as supplemented by the original claims.

Listing of Claims:

Claims 1-5 (canceled)

6. (currently amended) A method for protecting a digital signal, comprising the steps of:

providing a digital signal comprising digital data and file format information defining how the digital signal is encoded;

creating a predetermined key [[that]] to manipulate[[s]] [[the file format information]] the digital signal; and

manipulating the [[file format information]] digital signal using the predetermined key to generate at least one permutation of the digital signal parameterized by the file format information defining how the digital signal is encoded.

7. (original) The method of claim 6, wherein the digital signal represents a continuous analog waveform.

8. (original) The method of claim 6, wherein the predetermined key comprises a plurality of mask sets.

9. (original) The method of claim 6, wherein the digital signal is a message to be authenticated.

10. (previously presented) The method of claim 6, wherein the predetermined key comprises a key pair comprising a public key and a private key.

11. (original) The method of claim 6, further comprising the step of: using a digital watermarking technique to encode information that identifies ownership, use, or other information about the digital signal, into the digital signal.

12. (original) The method of claim 6, wherein the digital signal represents a still image, audio or video.

13. (previously presented) The method of claim 6, wherein the predetermined key comprises one or more mask sets having random or pseudo-random series of bits, the method further comprising the step of:

validating the one or more mask sets before manipulating the file format information using the predetermined key.

14. (previously presented) The method of claim 6, wherein the predetermined key comprises one or more mask sets having random or pseudo-random series of bits, the method further comprising the step of:

validating the one or more mask sets after manipulating the file format information using the predetermined key.

15. (previously presented) The method of claim 6, wherein the predetermined key comprises one or more mask sets having random or pseudo-random series of bits, the method further comprising the steps of:

generating a hash value using the one or more masks sets; and

authenticating the one or more mask sets by comparing the generated hash value with a predetermined hash value.

16. (previously presented) The method of claim 13, wherein said step of validating comprises the steps of:

generating a digital signature using the one or more mask sets; and

comparing the digital signature with a predetermined digital signature.

17. (previously presented) The method of claim 6, wherein the predetermined key comprises one or more mask sets having random or pseudo-random series of bits, the method further comprising the step of:

authenticating the one or more mask sets by comparing a generated digital signature with a predetermined digital signature.

18. (original) The method of claim 13, further comprising the step of:

using a digital watermarking technique to embed information that identifies ownership, use, or other information about the digital signal, into the digital signal; and

wherein said step of validating is dependent on validation of the embedded information.

19. (previously presented) The method of claim 6, further comprising the step of:

computing a secure one way hash function of data in the digital signal, wherein the secure one way hash function is insensitive to changes introduced into the digital signal during the step of file format manipulation.

20. (currently amended) A method for protecting a digital signal, comprising the steps of:

providing a digital signal comprising digital data and file format information describing how the digital signal is encoded;

creating a predetermined key comprising a mask set;

manipulating the [[file format information]] digital signal using the predetermined key wherein the manipulation is parameterized by the file format information describing how the digital signal is encoded;

authenticating the predetermined key during playback of the digital data; and

metering the playback of the digital data to monitor content.

21. (previously presented) The method of claim 20, wherein the predetermined key is authenticated to authenticate message information.

Claims 22-29 (canceled)

30. (currently amended) A method for protecting digital data, where the digital data is organized into a plurality of frames, each frame having i) a header comprising file format information and ii) at least a portion of the digital data, said method comprising the steps of:

creating a predetermined key to manipulate the file format information in one or more of the plurality of frames wherein the file format information defines how the digital data is encoded; and

manipulating the file format information using the predetermined key in at least two of the plurality of frames wherein the file format information defines how the digital data is encoded, such that the digital

data will be perceived by a human as noticeably altered if it is played without using a decode key to restore the file format information to a prior state.

31. (previously presented) The method of claim 30, wherein the predetermined key comprises a private key that is associated with a key pair.